(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 44 051 A 1**

(51) Int. Cl.[7]: **H 04 N 7/16**

(21) Aktenzeichen: 100 44 051.7
(22) Anmeldetag: 1. 9. 2000
(43) Offenlegungstag: 14. 3. 2002

DE 100 44 051 A 1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Schwenk, Jörg, Dr., 64807 Dieburg, DE; Saar, Eva, 64347 Griesheim, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 198 15 784 A1
US 55 55 308
WO 99 41 900 A1
BEUTELSPACHER,Albrecht, u.a.: Moderne Verfahren der Kryptographie, Vieweg, Braunschweig/Wiesbaden, 1998, 2. Aufl., ISBN 3-528-16590-1, S.69,71;
JP 10164550 A., In: Patent Abstracts of Japan;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zur Werbefinanzierung von Multimedia-Inhalten

(57) Die Werbeträger, welche die Darbietung von Nutzdaten finanzieren, sind daran interessiert, daß eingeblendete Werbeblöcke wirklich dargeboten und nicht durch Zwischenaufzeichnung übersprungen werden.
Um die Darbietung der Nutzdaten von der Wiedergabe der Werbeblöcke abhängig zu machen, werden in einige Stellen der Werbeblöcke Codeelemente eines Schlüssels eingebettet, die während des Abspielens der Werbeblöcke abgetastet und gesammelt und danach zu einem vollständigen Schlüssel verknüpft werden. Werden die nachfolgenden Nutzdaten mit diesem Schlüssel verschlüsselt, wird deren Wiedergabe vom Schlüssel abhängig.
Das vorgeschlagene Abhängigmachen der Wiedergabe der Nutzdaten von der Wiedergabe der Werbeblöcke kann sowohl beim bekannten werbefinanzierten Free-TV, bei bekannten und vorbereiteten Aufzeichnungsverfahren als auch für neue werbefinanzierte Multimedia-Inhalte und -Produkte verwendet werden.

DE 100 44 051 A 1

BUNDESDRUCKEREI 01.02 101 710/781/1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren der im Oberbegriff des Patentanspruchs 1 näher bezeichneten Art. Derartige Verfahren sind allgemein aus dem werbefinanzierten Free-TV bekannt und verbreitet und werden von Werbeträgern verwendet, welche die Darbietung von Nutzdaten mit der Darbietung von zeitweise eingeblendeten Werbeblöcken finanzieren wollen.

[0002] Die Verbreitung von Medien wird häufig über Werbeunterbrechungen finanziert. Dies ist heute im Fernsehbereich kein Problem, da der Kunde eine Sendung im Fernsehen nicht "vorspulen" kann. Dem Verhalten des "Zappens" wird von Seiten der Sender durch eine weitgehende Synchronisierung der Werbung Rechnung getragen.

[0003] Anders sieht es im Bereich aufgezeichneter Inhalte aus, z. B. bei Aufnahmen von Fernsehsendungen auf Videokassetten. Hier hat der Nutzer oft die Möglichkeiten, die Werbung zu umgehen, indem er einen Videofilm vorspult, bis die Werbung beendet ist. Dieses Problem tritt vor allem im Videobereich auf und ist auch für andere Medien (CD, DVD) denkbar.

[0004] Eine neue Dimension erhält das Problem mit einer Entwicklung, die von der Standardisierungsinitiative "TV Anytime" (http://www.tv-anytime.org/) gebündelt wird:

[0005] In Zukunft werden Fernseher, Videorecorder und/oder Set-Top-Boxen Speichermedien (z. B. Festplatten mit 50 bis 100 Gigabyte Kapazitäten) enthalten, die es ermöglichen, Inhalte ("Content") nach Herzenslust gleichzeitig aufzunehmen und wiederzugeben. Dadurch wird es für den Kunden um ein Vielfaches leichter, Werbepausen zu umgehen:

- Der Kunde zeichnet ca. 15 Minuten der Sendung auf.
- Dann beginnt er, diese anzuschauen.
- Wann immer eine Werbepause auftritt, überspringt er diese und setzt nach der Pause wieder an.

[0006] Der Schutz des "Content" war ein wichtiges Anliegen des DVD Standardisierungsgremiums (www.dvdforum.com). Daher wurde für DVD ein Verschlüsselungssystem (Content Scrambling System, CSS) spezifiziert. Nach diesem wird jedem Datenblock auf der DVD ein sogenannter "Header" vorangestellt, der den mit dem "disk key" verschlüsselten "title key" enthält. Mit diesem "title key" und einigen Zusatzbits kann dann der Inhalt der Nutzdaten (Content des Files) entschlüsselt werden.

[0007] Die Aufgabe der Erfindung ist es, ein Verfahren und dazu eine Vorrichtung aufzuzeigen, mit der sichergestellt werden kann, dass die Werbung tatsächlich abgespielt werden muss. (Der Kunde kann natürlich nicht gezwungen werden, diese auch anzusehen.) Mit dieser Methode werden auch neue Vermarktungsarten für durch Werbung finanzierte sogenannte "Content" möglich.

[0008] Die Erfindung löst diese Aufgabe mit den im Kennzeichen des Patentanspruchs 1 aufgeführten Verfahrensschritten.

[0009] Eine Vorrichtung, die zur Lösung dieser Aufgabe geeignet ist, ist im Kennzeichen des Patentanspruchs 6 beschrieben.

[0010] Vorteilhafte Aus- bzw. Weiterbildungen des Verfahrens sind in den Unteransprüchen 2 bis 5 beschrieben.

[0011] Nachfolgend wird die Erfindung anhand einiger Ausführungsbeispiele näher beschrieben.

[0012] Das Verfahren nach der Erfindung teilt einen Nutzinhalt ("Content" z. B. ein Film) in verschiedene Blöcke auf, die jeweils mit einem "title key" Schlüssel verschlüsselt

werden. Vor und zwischen diese Blöcke werden dann unverschlüsselte Werbeblöcke geschoben, die diesen Schlüssel enthalten. Ein Abspielgerät muß einen Großteil, möglichst sogar den ganzen Werbeblock abtasten ("scannen"), um an den Schlüssel zu gelangen. Dazu werden nachfolgend, ohne Anspruch auf Vollständigkeit, einige Varianten als Möglichkeiten der Realisierung aufgezeigt:

[0013] Die einfachste Möglichkeit besteht darin, den ganzen Schlüssel "title key" zu einem zufällig gewählten Zeitpunkt im Werbeblock zu verstecken. Das Abspielgerät muss dann im Mittel etwa die halbe Zeit des Werbeblocks abtasten ("scannen"), um ihn zu finden. Bereits eine Aufteilung des Schlüssels in zwei Codeelemente, die auf die erste und die zweite Hälfte des Werbeblockes an zufällige Zeitpunkte verteilt werden, zwingt zum "scannen" über einen längeren Zeitraum, der proportional der Aufteilung in mehr Codeelemente steigt.

[0014] Eine zweite Möglichkeit besteht in der Zerlegung des "title key"-Schlüssels mit sogenannten "Secret Sharing Schemes" in mehrere Teilgeheimnisse, die im Werbeblock versteckt werden. Das sind Schemas, bei denen man mehrere Teilgeheimnisse benötigt, die dann zu einem vollständigen Geheimnis zusammengesetzt werden. (Literatur: Beutelspacher, Schwenk, Wolfenstetter, "Moderne Verfahren der Kryptographie", Vieweg Verlag, 3. Auflage 2000)

[0015] Dieses Prinzip verlängert die notwendige Zeit zum Abtasten des Werbeblockes erheblich, indem in gewissen Abständen (z. B. in jedem Werbespot oder alle 10 Sekunden) während der Werbepause ein Teilgeheimnis in die Daten eingebracht wird. Diese Teilgeheimnisse werden während des Abspielens gesammelt, z. B. vom Abspielgerät.

[0016] Die folgenden Nutzdaten sind dann mit dem vollständigen Geheimnis als "title key" Schlüssel verschlüsselt und werden nur dann angezeigt, wenn ausreichend Teilgeheimnisse gesammelt wurden.

[0017] Unter welchen Bedingungen das der Fall ist, ist von dem verwendeten Secret Sharing Scheme abhängig. Denkbar sind Variationen, bei denen alles oder nur ein Teil der Werbung ablaufen muss, dabei kann ein Teil Pflicht, andere wahlweise sein.

[0018] Weitere Varianten des Verfahrens können hinsichtlich der Vollständigkeit der Codeelemente sinnvoll sein:

[0019] Die Variante, dass alle Teilgeheimnisse gesammelt werden müssen, ist nur sinnvoll bei vorbespielten Medien wie z. B. CD, DVD oder Videos. Hier kann sichergestellt werden, dass ein Abspielgerät auch wirklich alle Teilgeheimnisse empfangen kann.

[0020] Die zweite Variante besteht darin, dass k aus n Teilgeheimnisse gesammelt werden müssen.

[0021] Diese Variante empfiehlt sich für Rundfunksendungen, da sich hier ein Kunde ggf. später zuschalten kann und so keine Gelegenheit hat, die Teilgeheimnisse zu sammeln. Schaltet er sich erst nach der Werbepause zu, so muss er entweder eine gewisse "Strafzeit" warten, bis er außerhalb der Werbepause genug Teilgeheimnisse gesammelt hat, oder er ruft den Sitzungsschlüssel online bei einem Server ab. Wie die Teilgeheimnisse in die Daten eingebracht werden, hängt von dem Medium ab. Auch eine Realisierung mittels digitaler Wasserzeichen ist vorstellbar.

[0022] Eine weitere Variante besteht im Einfügen als digitale Zusatzinformation:

[0023] Hierbei werden die Teilgeheimnisse als spezielle Teile der Programm- Zusatzinformation auf digitaler Ebene dargestellt, z. B. als Teil der Service Information (SI) bei digitalem Fernsehen nach DVB, als Zusatzinformation im Datenteil von DVD (Entschlüsselung mittels CSS-Algorithmus) oder als eigene IP- Pakete bei IP-basierten Streaming-Anwendungen.

[0024] Eine weitere Variante besteht im Einfügen als Wasserzeichen Dabei werden die Daten als Wasserzeichen in den Inhalt ("Content") selber eingestellt. Dies verhindert ein Abtasten ("Scannen") der digitalen Zusatzinformationen mit Hilfsprogrammen. Der Aufwand eines solchen Scannens wäre äquivalent zum Darstellen des Contents, und es ergäben sich keine Vorteile.

[0025] Mit Hilfe der beschriebenen Erfindung können neue Produkte realisiert werden:

- Endgeräte für den Empfang bestimmter Kabelprogramme oder durch Werbung finanzierter Sendungen bzw. Abspielgeräte für Aufzeichnungen mit Werbeblöcken,
- Kostenlose Giveaway- DVD, -MPEG-CD, Audio-CD, die sich über Werbeeinlagen finanzieren. (Zum Beispiel eine DVD über die Geschichte des Radsports, die von Telekom-Werbeblöcken zum Team Telekom unterbrochen wird, als Geschenk in den T-Punkten. Oder der neue James Bond, bei dem bei jedem Auftreten eines BMW im Film der entsprechende Werbeblock zu diesem Modell eingeblendet wird.)
- Durch Werbung finanzierte Inhalte für TV-Anytime.

Patentansprüche

1. Verfahren zur Werbefinanzierung von Multimedia-Inhalten, die zwischen der Benutzung der Nutzdaten das Abspielen von Werbeblöcken enthalten, deren Träger die Benutzung der Nutzdaten finanzieren, **dadurch gekennzeichnet** dass
in einige Stellen der Werbeblöcke Codeelemente eines Schlüssels eingebettet werden,
diese Codeelemente eines Schlüssels während des Abspielens der Werbeblöcke abgetastet und gesammelt werden,
die Codeelemente schematisch zu einem vollständigen Schlüssel verknüpft werden,
die nachfolgenden Nutzdaten unter Nutzung des vollständigen Schlüssels verschlüsselt werden,
die Benutzung der Nutzdaten von einem vom Werbeträger zu bestimmenden Teil der Codeelemente bzw. vom vollständigen Schlüssel abhängig gemacht und ohne deren Erreichen gesperrt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Stellen in den Werbeblöcken wechselnd, bzw. zufällig gewählt werden.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass als Codeelemente Teilgeheimnisse eines Shared Secret Systems verwendet werden, die zu einem in seinem Umfang vorgegebenen vollständigen Geheimnis zusammengesetzt werden.

4. Verfahren nach Anspruch 1 bis 3, dadurch gekennzeichnet, dass die Schlüssel bzw. Teilgeheimnisse in den Werbeblöcken als spezielle Teile der Programm-Zusatzinformation auf digitaler Ebene dargestellt werden, insbesondere als Teil der Service-Information bei digitalem Fernsehen nach DVB, bzw. als Zusatzinformation im Datenteil von DVD, bzw. als eigene IP-Pakete bei IP-Anwendungen.

5. Verfahren nach Anspruch 1 bis 3, dadurch gekennzeichnet, dass der vollständige Schlüssel, bzw. dessen Codeelemente als Wasserzeichen in den Inhalt der Werbeblöcke eingestellt werden.

6. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 1 bis 5, dadurch gekennzeichnet, dass Endgeräte für die bevorzugte Wiedergabe gespeicherter bzw. gesendeter Werbeblöcke, insbesondere solche, die zu Vorzugsbedingungen vergeben werden, mit Entschlüsselungseinrichtungen versehen sind, welche das Sammeln der Codeelemente des Verfahrens beherrscht und mit einer Sperrschaltung verbunden sind, die den Nutzinhalt nur bei vollständiger Wiedergabe der Werbeblöcke freigeben.

- Leerseite -